Integer Solutions of Resultant Inequalities : a brief survey around results of Evertse (Number Theory from the Stand Point of Analytic Number Theroy [Theory])

数理解析研究所講究録
1091巻 1999年 112-118

Integer Solutions of Resultant Inequalities

a brief survey around results of Evertse

Noriko HIRATA-KOHNO

Department of Mathematics
College of Science and Technology
Nihon University
Suruga-dai, Kanda
Chiyoda, Tokyo 101-8308
JAPAN

本稿では、Resultant equations もしくは Resultant inequality と呼ばれるディオファントス不定方程式(不等式) についての、最近の J. H. Evertse などによる結果の、簡単な Survey を試みたいと思う。関連する自身の結果およびその周辺については、津田塾大学第4回整数論シンポジウム報告集にも述べたので、ここでは重複を避け、Resultant equations というものの一般論と、その整数解を求めることが Roth 型のディオファントス近似に帰着される理由について述べたい。

Definition

$f(X), g(X)$ を $\mathbf{Z}[X]$ の元とする。

$$f(X) = a_0X^r + a_1X^{r-1} + \cdots + a_r = a_0\prod_{i=1}^{r}(X-\alpha_i),$$

$$g(X) = b_0X^t + b_1X^{t-1} + \cdots + b_t = b_0\prod_{j=1}^{t}(X-\xi_j)$$

（ただし $a_0 \neq 0, b_0 \neq 0$）と書くとき、f と g の Resultant とは、サイズ $r+t$ の次の行列式である。

$$R(f,g) = \det \begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_r & & & \\ & a_0 & a_1 & \cdots & \cdots & a_r & & \\ & & \ddots & & & & \ddots & \\ & & & a_0 & a_1 & \cdots & \cdots & a_r \\ b_0 & b_1 & \cdots & b_t & & & & \\ & b_0 & b_1 & \cdots & b_t & & & \\ & & \ddots & & & \ddots & & \\ & & & \ddots & & & \ddots & \\ & & & & b_0 & b_1 & \cdots & b_t \end{pmatrix}$$

ここで $R(f,g) = a_0^t b_0^r \prod_{i=1}^r \prod_{j=1}^t (\alpha_i - \xi_j)$ であるので、f と g が共通根を持つときに限り $R(f,g) = 0$ となる。$R(f,g)$ をさらに書き換えると

$$R(f,g) = a_0^t \prod_{i=1}^r \left(b_0 \prod_{j=1}^t (X - \xi_j) \Big|_{X=\alpha_i} \right) = a_0^t \prod_{i=1}^r g(\alpha_i)$$

であることに注意する。

Mahler measure を定義する。$\mathbf{C}$ 上の多項式 $f(X) = a_0 \prod_{i=1}^r (X - \alpha_i)$ に対し

$$M(f) := |a_0| \prod_{i=1}^r \max(1, |\alpha_i|)$$

とおく。代数的数βに対してはその $\mathbf{Z}$ 上の最小多項式の Mahler measure をβの Mahler measure と定め、$M(\beta)$ と書く。

$h(\beta)$ を通常の logarithmic projective height とするとき、

$$h(\beta) = \frac{1}{[\mathbf{Q}(\beta) : \mathbf{Q}]} \log M(\beta)$$

が知られているので、$H(\beta) := \exp(h(\beta))$ に対しては、あるいはクラシカルな高さ（βの最小多項式の係数の絶対値の最大値）に対しては、

$H(\beta) \asymp M(\beta)$、 $d = [\mathbf{Q}(\beta) : \mathbf{Q}]$ となっている。

$f(X) \in \mathbf{Z}[X]$ を degree r の多項式とし、固定する。正整数 t も固定する。$f(X)$ は与えられた多項式、$g(X)$ を未知多項式、すなわち、$g(X)$ の係数 $b_0, b_1, \cdots, b_t$ を未知整数とみなす。

κを正実数とする。次のディオファントス不定不等式を Resultant inequality と呼ぶ。

$$(1) \qquad 0 < |R(f,g)| < M(g)^{r-\kappa}$$

E. Wirsing [Wi] は、fが重根を持たないとき、仮定

$$\kappa > 2t(1 + \frac{1}{3} + \cdots + \frac{1}{2t-1})$$

のもとで、(1) の解 $g(X)$ は有限個であることを示した。W. M. Schmidt [S1] は、fが重根を持たず、さらに次数 t 以下の irreducible factor を $\mathbf{Z}[X]$ に持たないならば、仮定$\kappa > 2t$ のもとで、(1) の解 $g(X)$ は有限個であることを証明した。さらに、fが重根を持たないとき、仮定$\kappa > 2t$ のもとで、(1) の解 $g(X)$ が有限個であることは、Schmidt の部分空間定理の応用により得られる M. Ru-P. M. Wong の定理から次のようにして示されることが [E1] に述べられている。

Ru-Wong の定理 [R-Wo]

$q \geq 2n-1$ とする。$L_1, \cdots, L_q$ を$\overline{\mathbf{Q}}$ 係数の n 変数 1 次形式 で、一般の位置にあるものとする。このとき$\varepsilon > 0$ に対し、次の不定不等式をみたす、$L_1, \cdots, L_q$の零点以外の整数解 $\mathbf{x} \in \mathbf{Z}^n$ は有限個である ：

$$\prod_{i=1}^{q} \frac{|L_i(\mathbf{x})|}{|\mathbf{x}|} < \frac{1}{|\mathbf{x}|^{2n-2+\varepsilon}}.$$

ただし $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbf{Z}^n$ に対し、$|\mathbf{x}| = (|x_1|^2 + \cdots + |x_n|^2)^{\frac{1}{2}}$ とする。

Ru-Wong　から (1) の有限性を導く証明

[E1] にも言及されており、もともと [S1 の議論を用いているのだが、$r < 2t+1$ のときについては、筆者は [E2] に注意された。

$B = (b_0, b_1, \cdots, b_t) \in \mathbf{Z}^{t+1}$ を　$g(X)$ の未知係数からなるベクトルとおき、$L_i(B) = \alpha_i^t b_0 + \alpha_i^{t-1} b_1 + \cdots + b_t (1 \leq i \leq r)$ とする。つまり、$\alpha_i^t, \alpha_i^{t-1}, \cdots 1$ たちは、与えられた L_i の係数であると見なす。$q = r$ とす

る。このとき、$L_i (1 \leq i \leq r)$ が一般の位置にあることは、fが重根を持たないので、Van der Monde 行列式

$$\det \begin{pmatrix} \alpha_1^t & \cdots & \cdots & \alpha_1 & 1 \\ \cdot & \cdots & \cdots & \cdot & \cdot \\ \alpha_t^t & \cdots & \cdots & \alpha_t & 1 \end{pmatrix} \neq 0$$

よりわかる [E2]。

$R(f,g) = a_0^t L_1(B) \cdots L_r(B)$ であるから、$q = r \geq 2(t+1)-1 \quad (n = t+1)$ のとき、つまり $r \geq 2t+1$ のときには、Ru-Wong の上述の定理の不等式においてεのかわりにε'をとりなおした

$$\prod_{i=1}^{r} \frac{|L_i(\mathbf{x})|}{|L_i||\mathbf{x}|} < \frac{1}{|\mathbf{x}|^{2n-2+\varepsilon'}}$$

（ここで、$|L_i|$は、L_iの係数ベクトルのユークリッドノルムとする）を考えることによっても有限性は同じであることから、(1) は有限個の解を持つことが確かめられる。

$$\frac{|L_i(\mathbf{x})|}{|L_i||\mathbf{x}|} \leq 1$$

であることに注意すると、$r < 2t+1$ に対しては、不等式

$$\prod_{i=1}^{r} \frac{|L_i(\mathbf{x})|}{|L_i||\mathbf{x}|} < \frac{1}{|\mathbf{x}|^{2n-2+\varepsilon'}}$$

の解は、

$$\prod_{i=1}^{2t+1} \frac{|L_i(\mathbf{x})|}{|L_i||\mathbf{x}|} < \frac{1}{|\mathbf{x}|^{2n-2+\varepsilon'}}$$

の解の部分集合であるから、有限個となり、解の個数は同じ、もしくは少なくなる [E2]。

(1) についての quantitative result としては、J. -H. Evertse の結果 [E1] があるが、Gap Principle の確立のために、$g(X)$ には、より強い条件 irreducible であることを課し、また、仮定$\kappa > 2t(1 + \frac{1}{3} + \cdots + \frac{1}{2t-1})$ であるときのみに限っている。したがってκについては Schmidt、Ru-Wong の条件よりも強い。

Roth 型の拡張のディオファントス近似から、(1) の有限性を導く

さて、ここで Roth 型の拡張ともいえる次のディオファントス近似 (2) を考えて、以下に (1) の有限性が (2) から導かれることを示そう。

$| x, y |= \max(| x |, | y |)$ という記号を定める。ある正実数$\varphi_1, \cdots, \varphi_t$ と$\alpha_1, \cdots, \alpha_t \in \overline{\mathbf{Q}}$ (これは、Resultant Inequality に出てくるα_i とは限らない) および、未知数として $\mathbf{Q}$ 上 t 次の代数的数ξ(この conjugates を $\xi^{(1)}, \cdots, \xi^{(t)}$ と書く) に対してディオファントス近似不等式

$$(2) \qquad | \alpha_i - \xi^{(i)} |< \frac{1}{M(\xi)^{\varphi_i}} \ (1 \leq i \leq t)$$

を考える。

Wirsing [Wi] は、(2) が、

$$(3) \qquad \max_I (\# I)^2 > 2t \left(\sum_{i \in I} \varphi_i^{-1} \right)$$

(max は、$\{i \in \{1 \cdots t\} : \varphi_i \neq 0\}$ のすべての non-empty subsets を走る) を満たすときに、代数的数の解ξは有限個であることを示した。Evertse は、この定量的結果を与えた [E1]。この (2) の不等式の解の有限性から、(1) の解の有限性が出ることを説明したい [E1]。

$$(4) \qquad \frac{|R(f, g)|}{M(f)^t M(g)^r} = \prod_{i=1}^{t} \prod_{j=1}^{r} \frac{|\alpha_j - \xi^{(i)}|}{|1, \alpha_j| \ |1, \xi^{(i)}|}$$

である。次数 t の algebraic number ξ に対し、$\mathbf{Q}$ 上の conjugates $\xi^{(1)} \cdots \xi^{(t)}$ が順序

$$\min_{1 \leq j \leq r} \frac{|\alpha_j - \xi^{(1)}|}{|1, \alpha_j|} \leq \cdots \leq \min_{1 \leq j \leq r} \frac{|\alpha_j - \xi^{(t)}|}{|1, \alpha_j|}$$

を満たすとする。

α_{j_i}を各 $1 \leq i \leq t$ に対し

$$\frac{|\alpha_{j_i} - \xi^{(i)}|}{|1, \alpha_{j_i}|} = \min_{1 \leq j \leq r} \frac{|\alpha_j - \xi^{(i)}|}{|1, \alpha_j|}$$

となる fの根とする（ここでα_{j_i}たちは、t個になった）。

三角不等式より $j \neq j_i$ において

$$\frac{|\alpha_j - \xi^{(i)}|}{|1,\alpha_j|\ |1,\xi^{(i)}|} \geq \frac{|\alpha_{j_i} - \alpha_j|}{2|1,\alpha_{j_i}|\ |1,\alpha_j|}$$

が成り立つことと、discriminant の定義 $D(f) = a_0^{2r-2}\prod_{1\leq p<q\leq r}(\alpha_p - \alpha_q)^2 \in \mathbf{Z} - \{0\}$ （fは重根なし）に注意すると、

$$\prod_{j\neq j_i} \frac{|\alpha_{j_i} - \alpha_j|}{2|1,\alpha_{j_i}|\ |1,\alpha_j|} \geq \prod_{1\leq p<q\leq r} \frac{|\alpha_p - \alpha_q|}{2|1,\alpha_p|\ |1,\alpha_q|}$$

$$= \frac{|D(f)|^{\frac{1}{2}}}{2^{\frac{r(r-1)}{2}} M(f)^{r-1}}$$

だから、$D(f)$、$M(f)$、rとt で書ける定数Cに対して

$$\frac{|R(f,g)|}{M(f)^t M(g)^r} \geq C^{-1} \prod_{i=1}^{t} \frac{|\alpha_{j_i} - \xi^{(i)}|}{2|1,\alpha_{j_i}|\ |1,\xi^{(i)}|}$$

となる。$M(g) = M(\xi)$ なので、(4) の 1 から rまでの積の中の各分数は 2 以下であることに注意すると、(1)(2) より、ときたい不等式は、定数 C'に対して

$$\prod_{i=1}^{t} \frac{|\alpha_{j_i} - \xi^{(i)}|}{2|1,\alpha_{j_i}|\ |1,\xi^{(i)}|} < \frac{C'}{M(\xi)^{\kappa}}$$

となるが、Evertse の combinatorical lemma [E1] を用いると

$$\frac{|\alpha_{j_i} - \xi^{(i)}|}{2|1,\alpha_{j_i}|\ |1,\xi^{(i)}|} \leq \frac{1}{M(\xi)^{\varphi_i}}$$

に分けられる正実数φ_iで、諸条件をみたすものが存在することがわかる。このことから、(1) の解は、(2) （の左辺を変形したものだが、φ_i より少し小さいφ_i' を取り直せばよい）の解に含まれる。

References

[E1] J. -H. Evertse, *The number of algebraic numbers of given degree approximating a given algebraic number*, London Math. Soc. Lecture Notes Series 247, ed. Y. Motohash (1997), Cambridge, pp 53-83.

[E2]-, *personal communication*, December, 1998.

[R-Wo] M. Ru-P. M. Wong, *Integral points of* $\mathbf{P}^n \backslash \{2n+1$ *hyperplanes in general position*$\}$, Invent. Math. 106 (1991), 195-216.

[S1] W. M. Schmidt, *Inequalities for Resultants and for Decomposable Forms*, Proceedings of the Conference : Diophantine Approximation and its Applications, ed. C. Osgood, Academic Press (1973), pp 235-253.

[S2] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Math. 785 (1980), Springer.

[Wi] E. Wirsing *On approximations of algebraic numbers by algebraic numbers of bounded degree*, Proc. Symp. Pure Math. 20, ed. D. J. Lewis, AMS (1971), pp 213-248.